



Centers for Medicare & Medicaid Services

# **CMS Enterprise Portal Quick Reference Guide (QRG)**

## **Help Desk Multi-Factor Authentication (MFA) Support**

---

August 19, 2016  
Version 1.2 Final



**Table of Contents**

1. Introduction \_\_\_\_\_ 2

2. Step-by-Step Instructions to Unlock a Registered MFA Device \_\_\_\_\_ 3

3. Step-by-Step Instructions to Remove a Registered MFA Device \_\_\_\_\_ 10

4. Step-by-Step Instructions to Generate One-Time Security Code \_\_\_\_\_ 17

### 1. Introduction

This guide provides step-by-step instructions on how Application Help Desks can support their users for the following Multi-Factor Authentication (MFA) related services:

- Unlock MFA device(s)
- Remove MFA device(s)
- Generate a One-Time Security Code

**Note:** This document assumes that the application user has an active CMS Enterprise Portal account, a role in <Application Name>, and has registered for MFA in order for the Application Help Desk to provide support.

#### Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is a security mechanism that is implemented to verify the legitimacy of a person or transaction.

MFA requires you to provide more than one form of verification in order to prove your identity. MFA registration is required only once when you are requesting a role, but will be verified every time you log into the CMS Enterprise Portal.

During the MFA registration process, the CMS Enterprise Portal requires registration of a phone, computer, or e-mail to add an additional level of security to a user's account.

You may select from the following options to complete the registration process:

- **Smart Phone:** Download Validation and Identity Protection (VIP) access software on your smart phone/tablet. You must enter the alphanumeric credential ID that is generated by the VIP access client. You will then enter the Security Code generated by the VIP client.
- **Computer:** Download VIP access software on your computer. You must enter the alphanumeric credential ID generated by the VIP access client. You will enter the Security Code generated by the VIP client.
- **E-mail:** Select the e-mail option to receive an e-mail containing a Security Code required at login. You must provide a valid, accessible e-mail address.
- **Short Message Service (SMS):** Use the SMS option to have your Security Code texted to your phone. You must enter a valid phone number. The phone must be capable of receiving text messages. Carrier charges may apply.
- **Interactive Voice Response (IVR):** Select the IVR option to receive a voice message containing your Security Code. You must provide a valid phone number and (optional) phone extension.

For registering MFA devices, refer to the following EIDM Quick Reference Guides:


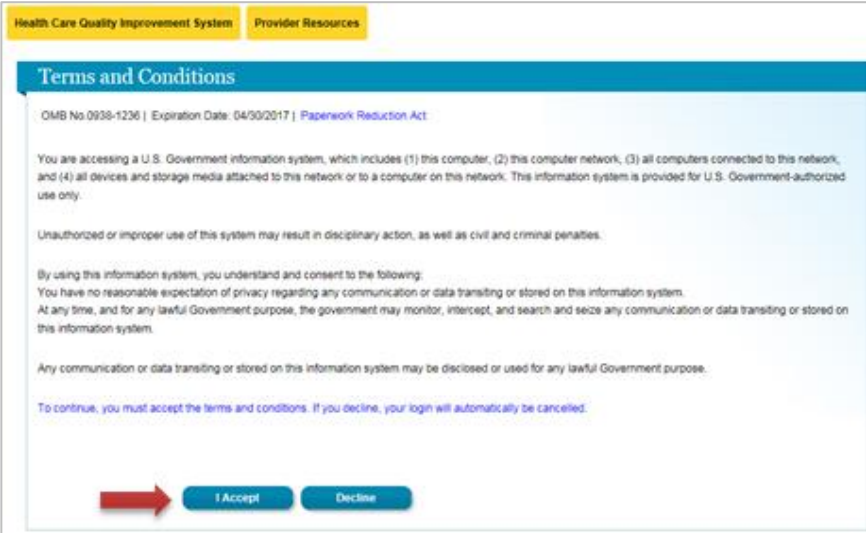
- EIDM QRG – Users Adding MFA to Application Role
- EIDM QRG – User Login

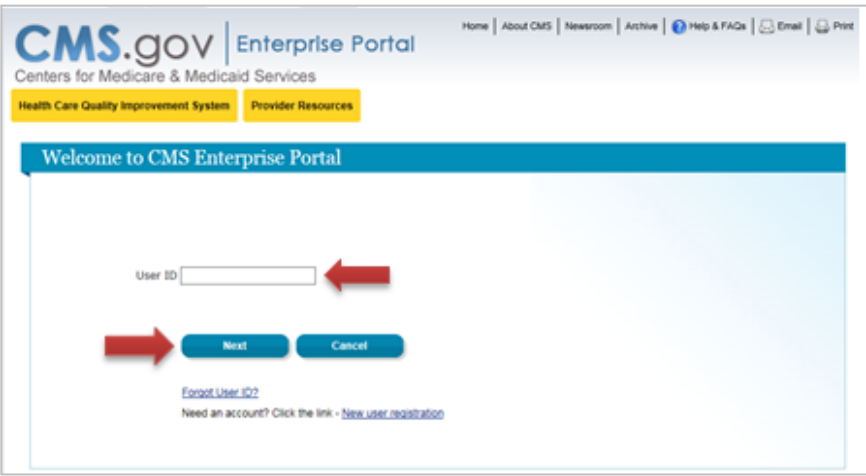
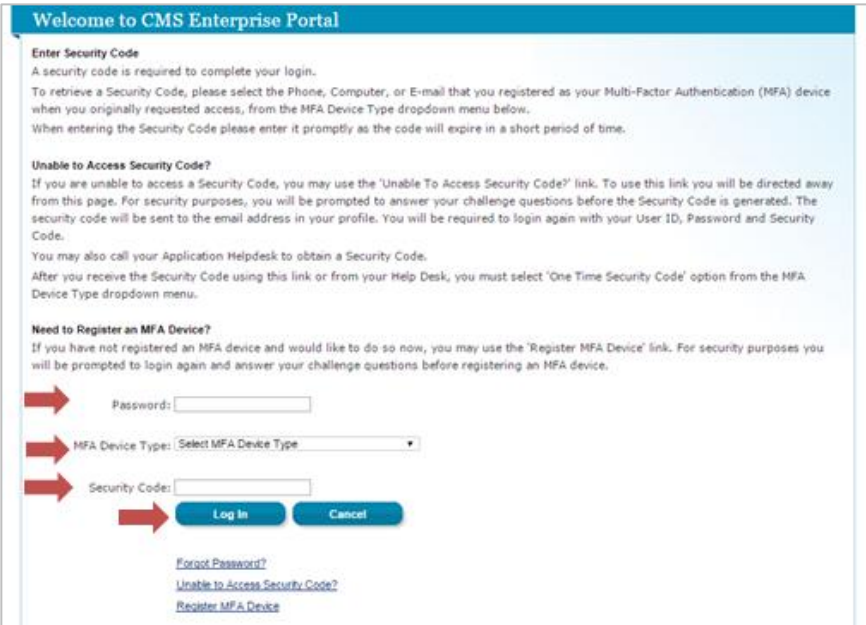
For accessing the 'User Details' page, refer to the following EIDM Quick Reference Guides:

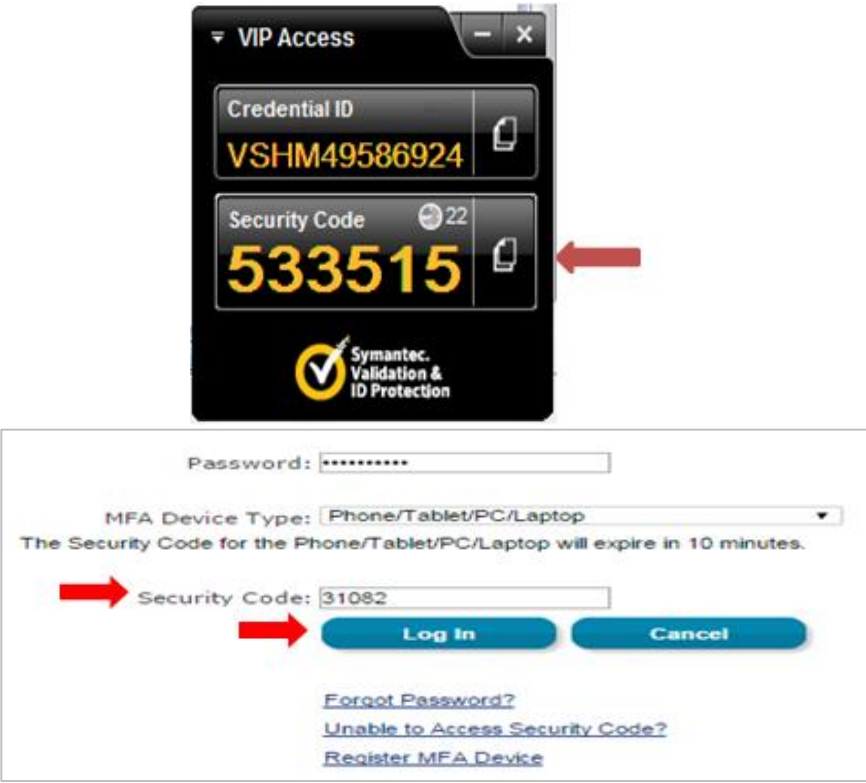
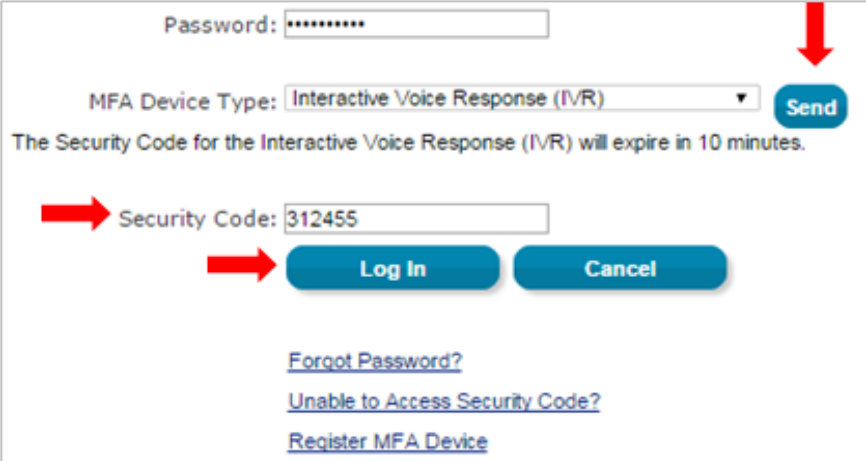
- EIDM QRG – Help Desk Manual LOA Update

## 2. Step-by-Step Instructions to Unlock a Registered MFA Device

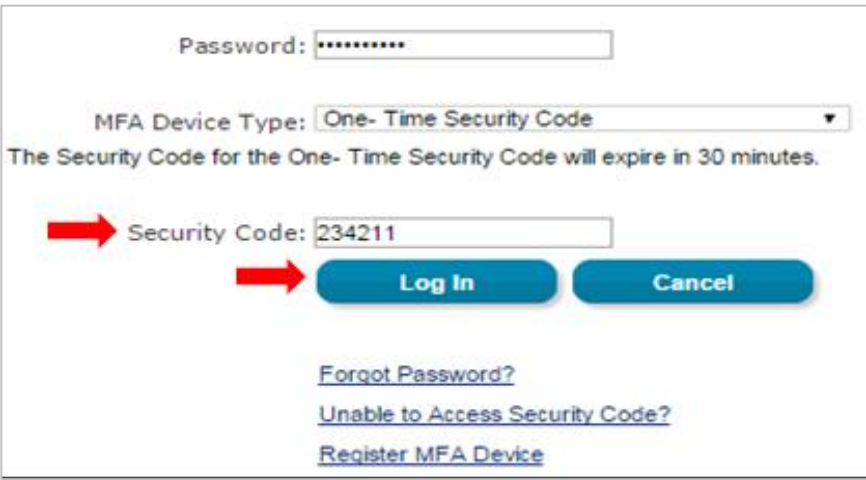
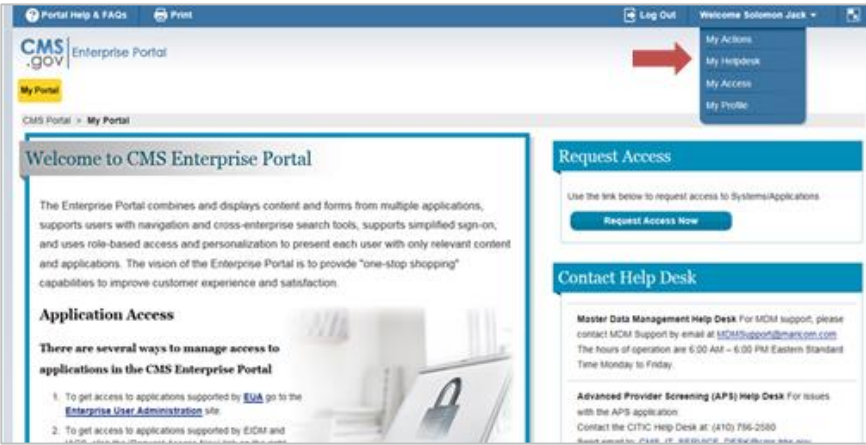
This section outlines the steps Application Help Desk Users, Application Approvers, and EIDM Help Desk Users take to unlock a registered phone, computer, or e-mail address. Please follow each step listed below unless otherwise noted.

Steps	Screenshots
<p>1. Go to <a href="https://portal.cms.gov/">https://portal.cms.gov/</a> and select <b>Login to CMS Secure Portal</b> on the CMS Enterprise Portal.</p> <p><i>Note: The CMS Enterprise Portal supports the following browsers: Internet Explorer 11, Firefox, Chrome, and Safari.</i></p>	
<p>2. Read the 'Terms and Conditions' page and select <b>I Accept</b> to continue.</p>	

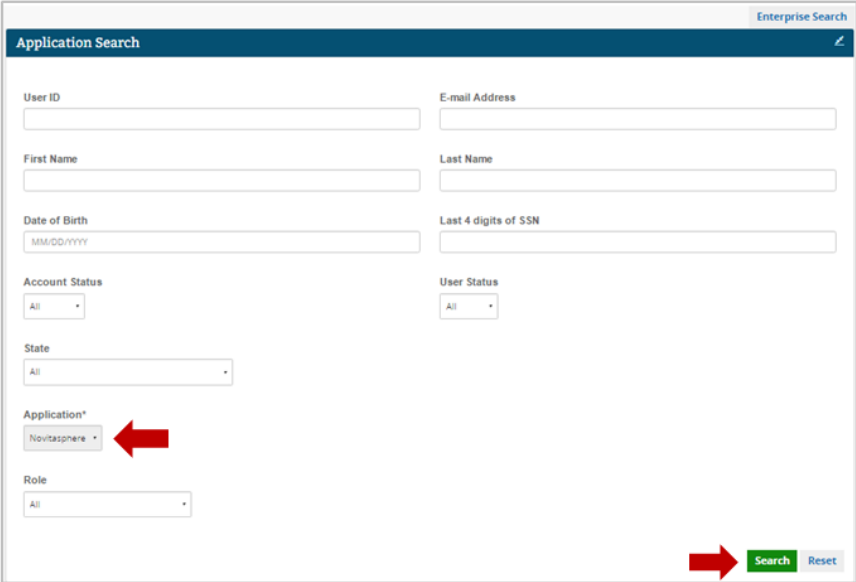
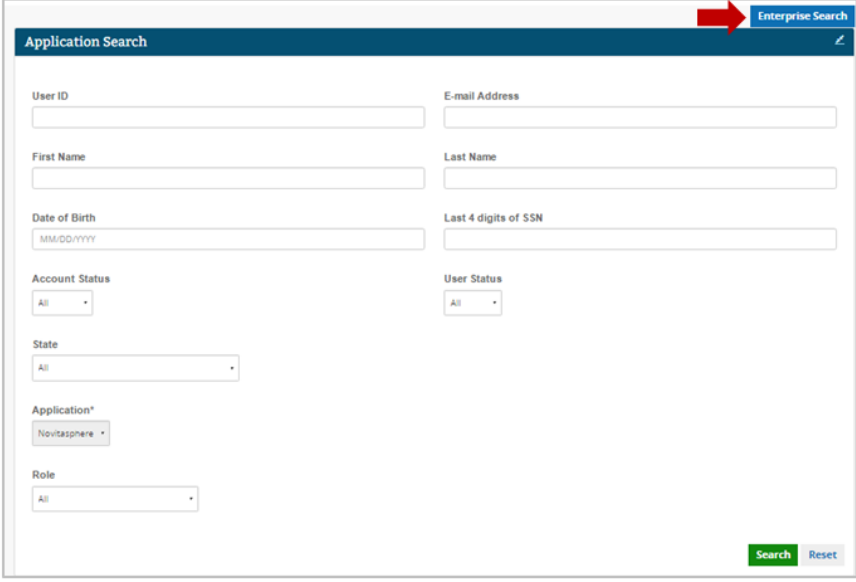
Steps	Screenshots
<p>3. Enter your <b>User ID</b> and select <b>Next</b>.</p>	
<p>4. Enter your <b>Password</b>, select an <b>MFA Device Type</b> from the drop-down, enter the <b>Security Code</b>, and select <b>Log In</b>.</p> <p><i>Note: The 'Security Code' for the 'E-mail' and 'One-Time Security Code' options expires after 30 minutes. The 'Security Code' for the other MFA device types expires after 10 minutes. If you are unable to enter the code within the period, you will need to request a new one.</i></p> <p><i>If you do not have access to your registered MFA device, please refer to the 'User Login' QRG for step-by-step instructions on how to register an MFA Device.</i></p>	

Steps	Screenshots
<p>4a. If you select <b>Phone/Tablet/PC/Laptop</b> as the 'MFA Device Type', enter the VIP Access software's 'Security Code' as the MFA <b>Security Code</b> and select <b>Log In</b>.</p>	
<p>4b. If you select <b>Text Message – Short Message Service (SMS)</b>, <b>Interactive Voice Response (IVR)</b>, or <b>E-mail</b> as the 'MFA Device Type', select <b>Send</b> to receive the code on the selected MFA device type.</p> <p>Enter the code in the <b>Security Code</b> field and select <b>Log In</b>.</p>	

## CMS Enterprise Portal QRG for Help Desk MFA Support

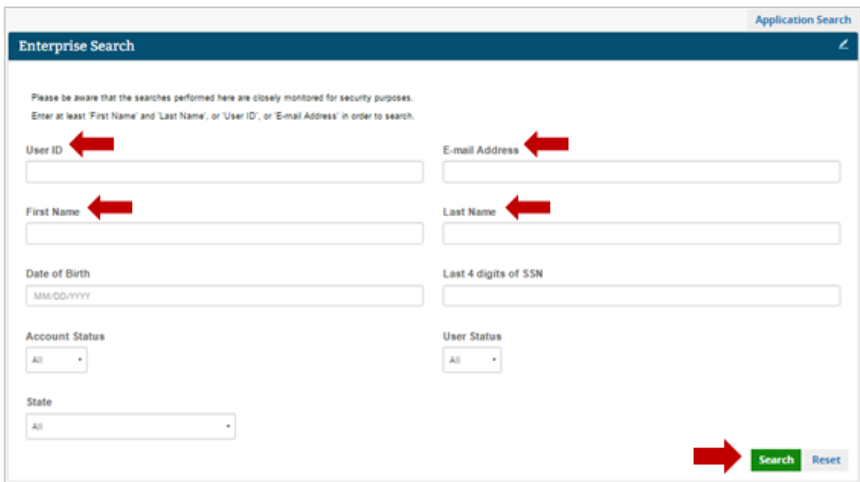
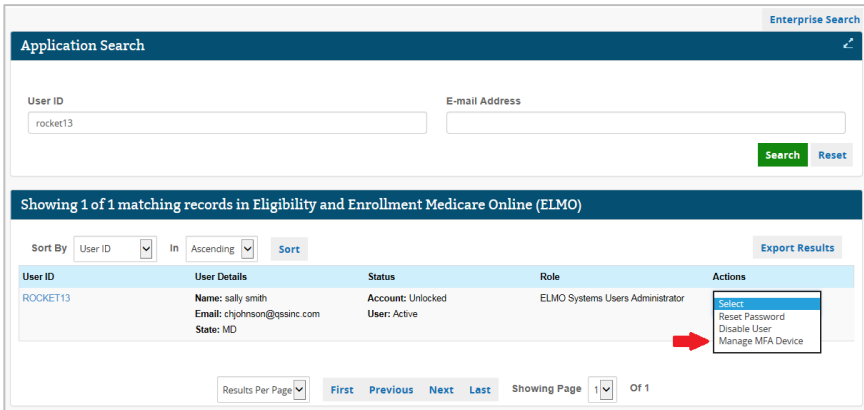
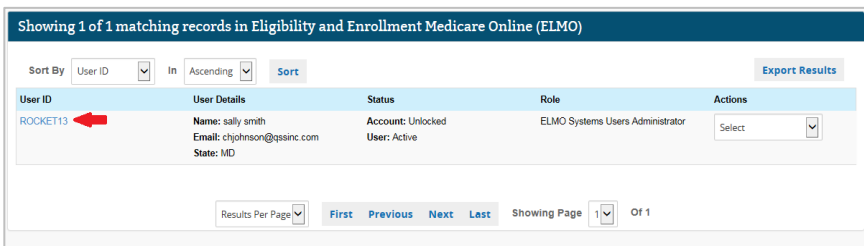
Steps	Screenshots
<p>4c. If you select <b>One-Time Security Code</b> as the 'MFA Device Type', enter the code you receive either in the e-mail sent to your registered e-mail address via the 'Unable to Access Security Code?' link or from your Application Help Desk in the <b>Security Code</b> field and select <b>Log In</b>.</p>	
<p>5. Locate the 'Welcome &lt;First&gt; &lt;Last&gt;' drop-down list in the top-right corner of the page and select <b>My Helpdesk</b>.</p>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

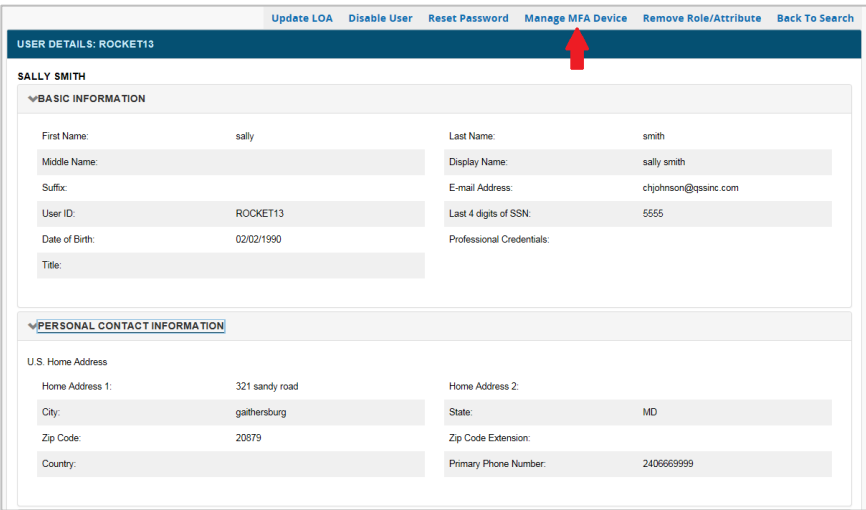
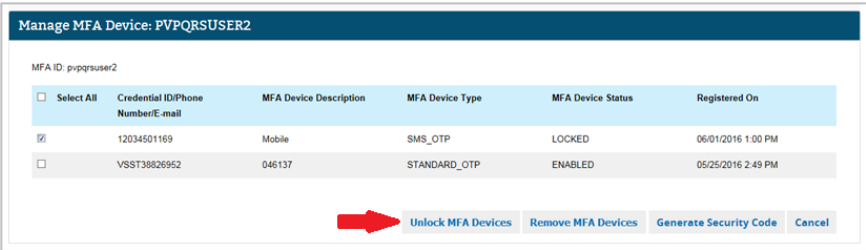
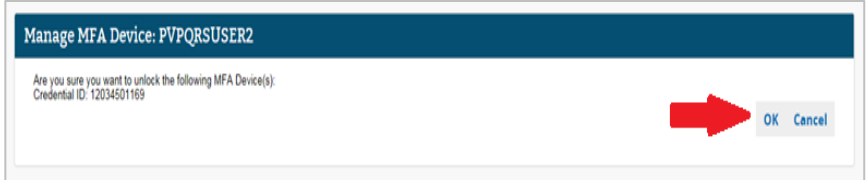
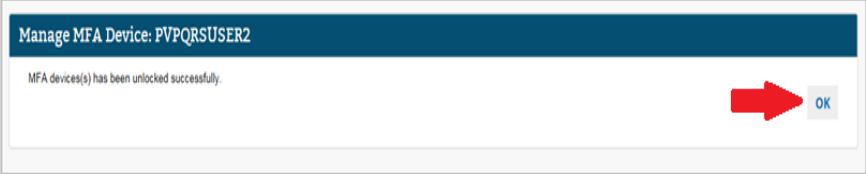
Steps	Screenshots
<p>6. Enter the user's details on the 'Application Search' page and select <b>Search</b>.</p> <p><i><b>Note:</b> Use this to search and manage user accounts under your authority. You must select at least the <b>Application</b> to perform a search. Only the first 1,000 results will display.</i></p>	
<p>6a. If you are unable to locate a user in 'Application Search', you can select 'Enterprise Search', enter the user's details, and select <b>Search</b>.</p> <p><i><b>Note:</b> Use this to search and manage user accounts in the CMS Enterprise Portal. This search option is intended for helping users who may have called the wrong Help Desk or may not have an application role, etc. You must enter at least the <b>User ID</b> (or) <b>E-mail Address</b> (or) a combination of <b>First Name</b> (and) <b>Last Name</b> to perform a search. The results will only display if 10 or fewer results match the criteria.</i></p>	



## CMS Enterprise Portal QRG for Help Desk MFA Support


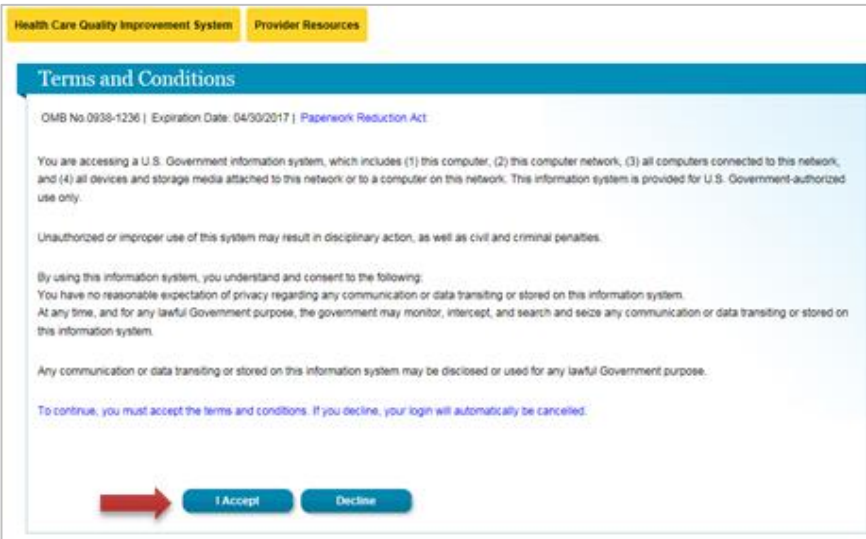
Steps	Screenshots
	
<p>7. Select <b>Manage MFA Device</b> from the 'Actions' drop-down list.</p> <p><i>Note: The option to select 'Manage MFA Device' is also available on the 'User Details' page.</i></p>	
<p>7a. Select the <b>User ID</b> to go to the 'User Details' page.</p>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

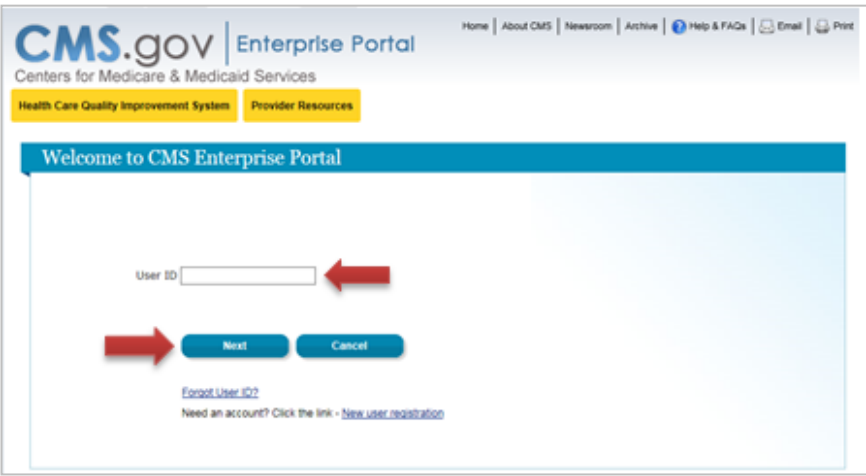
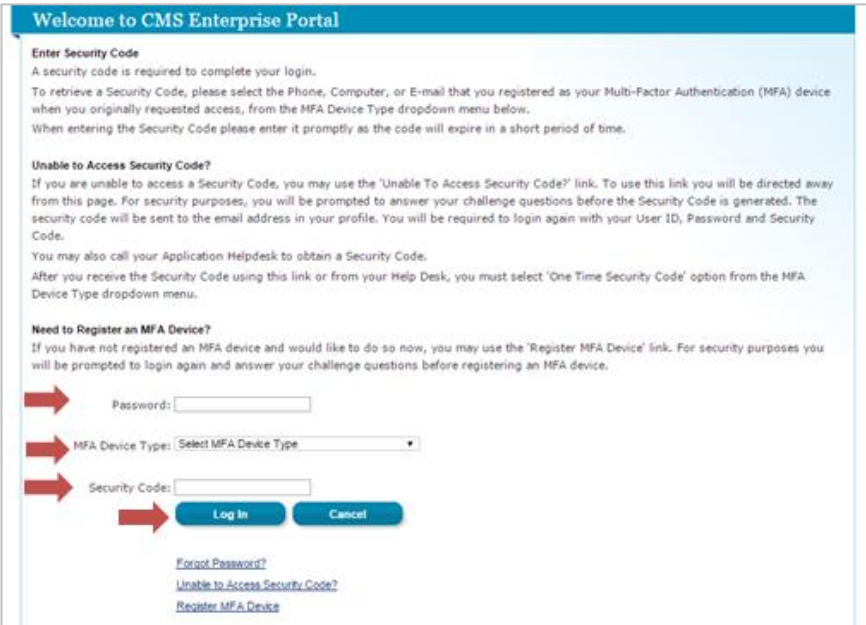
Steps	Screenshots
7b. Select <b>Manage MFA Device</b> .	
<p>8. Select the checkbox corresponding to the locked MFA device and select <b>Unlock MFA Devices</b>.</p> <p><i>Note: The option to <b>Unlock MFA Devices</b> is enabled only if there is an MFA device for the user with the locked status.</i></p>	
<p>9. Select <b>OK</b> to confirm unlocking the registered MFA device.</p> <p>OR</p> <p>Select <b>Cancel</b> to return to the 'Manage MFA Device' page.</p> <p><i>Note: If the selected device(s) is already in Enabled status, an error message will be displayed.</i></p>	
10. A success message displays. Select <b>OK</b> to return to the search results.	

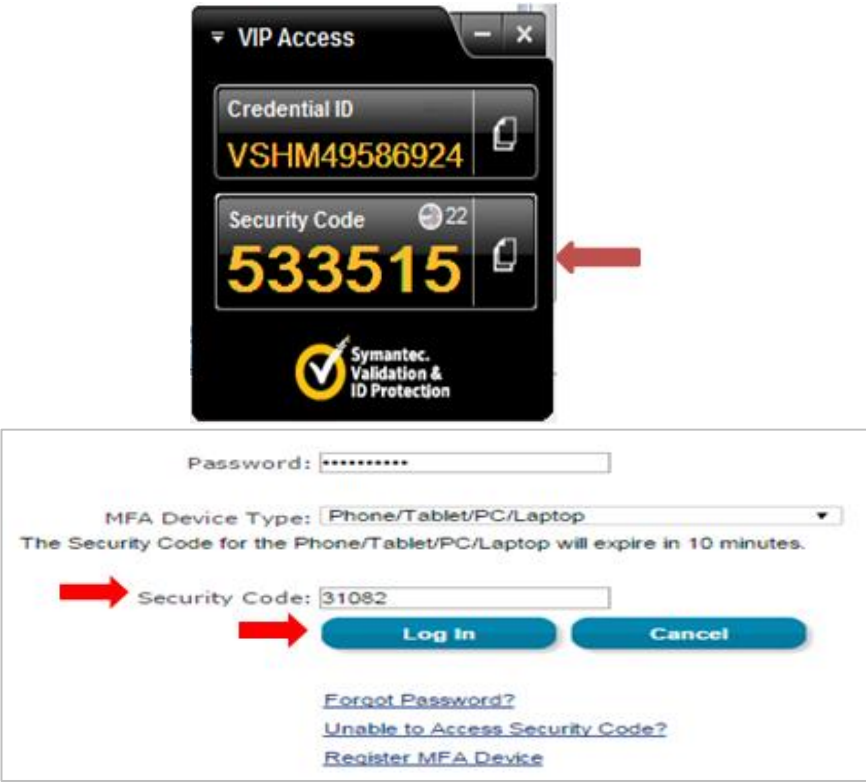
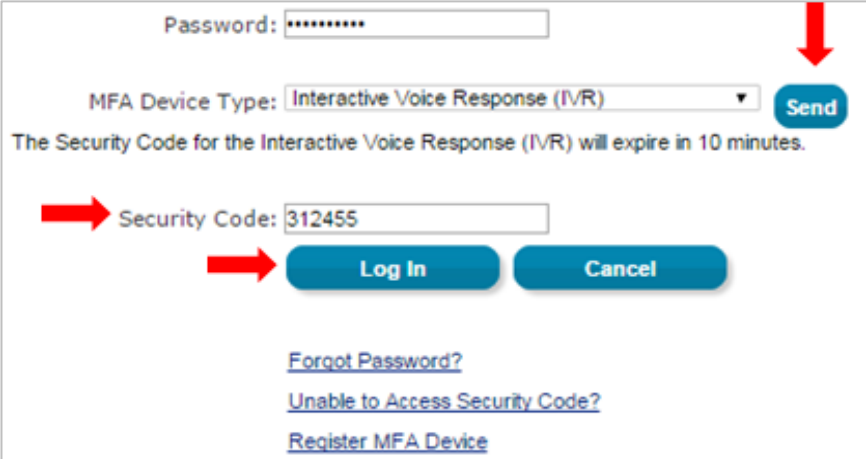
## 3. Step-by-Step Instructions to Remove a Registered MFA Device

This section outlines the steps Application Help Desk Users, Application Approvers, and EIDM Help Desk Users take to unlock a registered phone, computer, or e-mail. Please follow each step listed below unless otherwise noted.

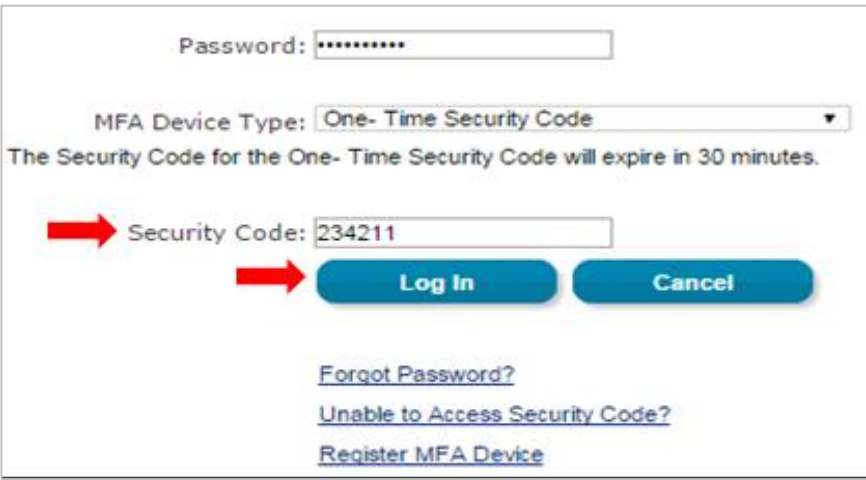
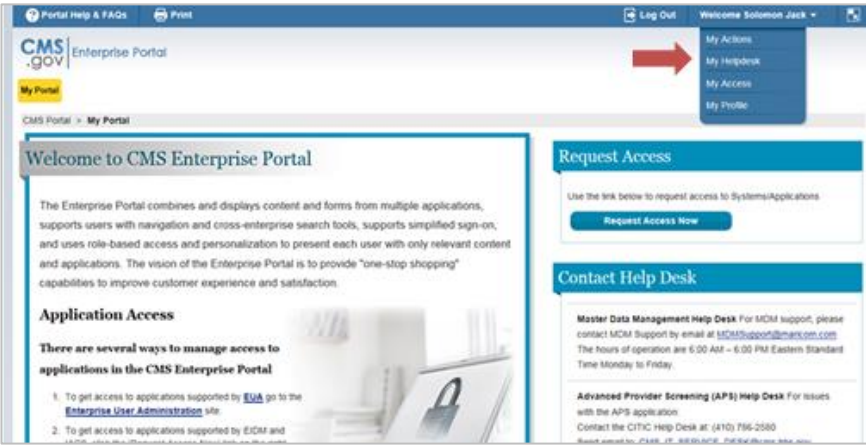
Steps	Screenshots
<p>1. Go to <a href="https://portal.cms.gov/">https://portal.cms.gov/</a> and select <b>Login to CMS Secure Portal</b> on the CMS Enterprise Portal.</p> <p><i>Note: The CMS Enterprise Portal supports the following browsers: Internet Explorer 11, Firefox, Chrome, and Safari.</i></p>	
<p>2. Read the 'Terms and Conditions' page and select <b>I Accept</b> to continue.</p>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

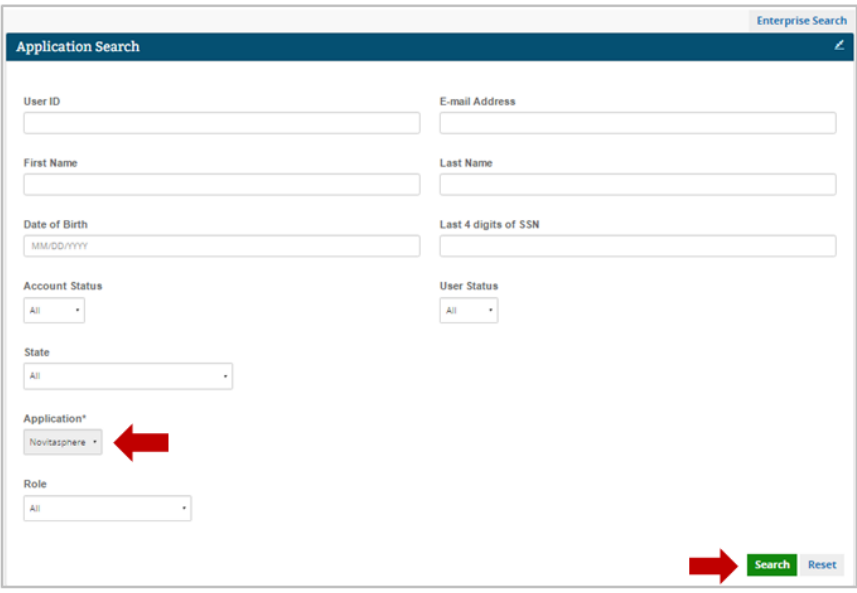
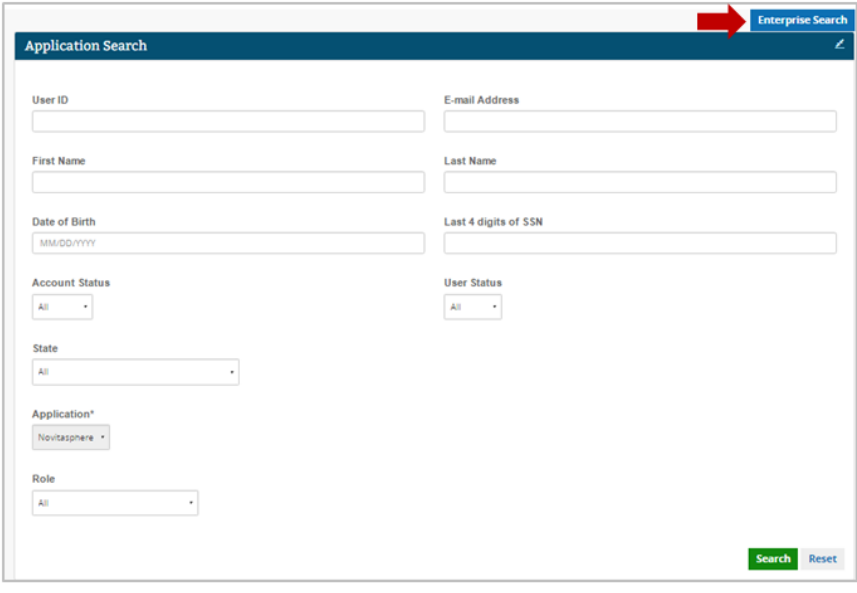
Steps	Screenshots
<p>3. Enter your <b>User ID</b> and select <b>Next</b>.</p>	
<p>4. Enter your <b>Password</b>, select an <b>MFA Device Type</b> from the drop-down list, enter the <b>Security Code</b>, and select <b>Log In</b>.</p> <p><i>Note: The 'Security Code' for the 'E-mail' and 'One-Time Security Code' options expires after 30 minutes. The 'Security Code' for the other MFA device types expires after 10 minutes. If you are unable to enter the code within the period, you will need to request a new one.</i></p> <p><i>If you do not have access to your registered MFA device, please refer to the 'User Login' QRG for step-by-step instructions on how to register an MFA Device.</i></p>	

Steps	Screenshots
<p>4a. If you select <b>Phone/Tablet/PC/Laptop</b> as the 'MFA Device Type', enter the VIP Access software's 'Security Code' as the MFA <b>Security Code</b> and select <b>Log In</b>.</p>	
<p>4b. If you select <b>Text Message – Short Message Service (SMS)</b>, <b>Interactive Voice Response (IVR)</b>, or <b>E-mail</b> as the 'MFA Device Type', select <b>Send</b> to receive the code on the selected MFA device type.</p> <p>Enter the code in the <b>Security Code</b> field and select <b>Log In</b>.</p>	

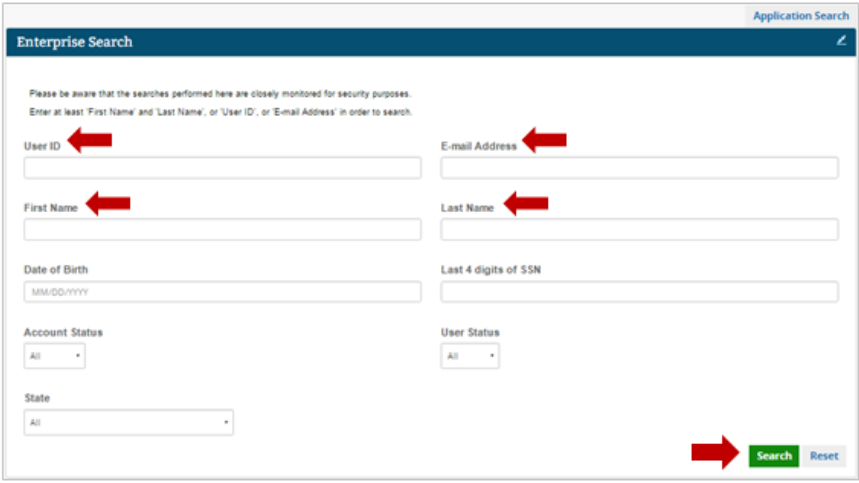
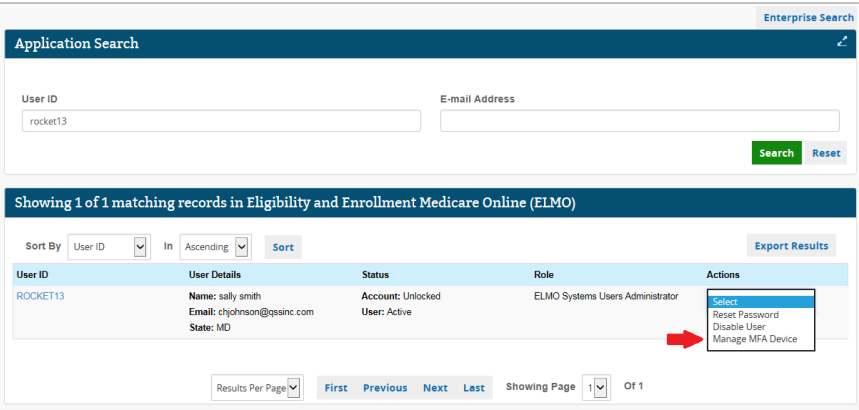
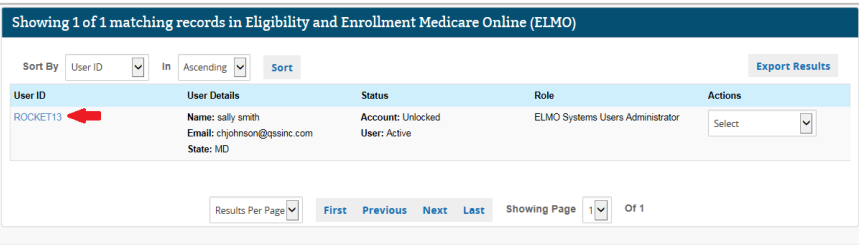
## CMS Enterprise Portal QRG for Help Desk MFA Support

Steps	Screenshots
<p>4c. If you select <b>One-Time Security Code</b> as the 'MFA Device Type', enter the code you receive either in the e-mail sent to your registered e-mail address via the 'Unable to Access Security Code?' link or from your Application Help Desk in the <b>Security Code</b> field and select <b>Log In</b>.</p>	
<p>5. Locate the 'Welcome &lt;First&gt; &lt;Last&gt;' drop-down list in the top-right corner of the page and select <b>My Helpdesk</b>.</p>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

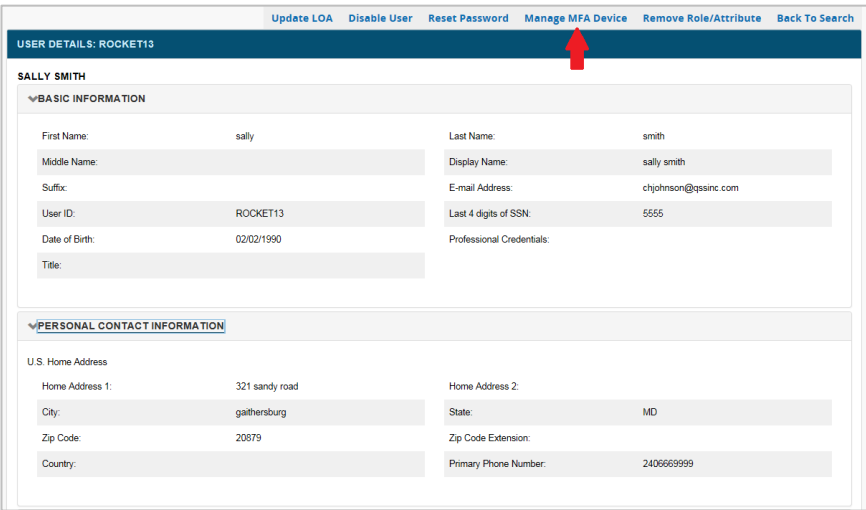
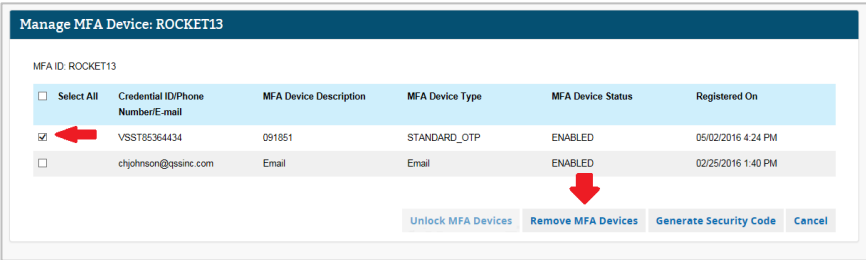

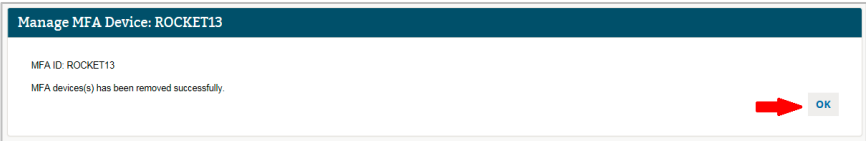
Steps	Screenshots
<p>6. Enter the user's details on the 'Application Search' page and select <b>Search</b>.</p> <p><i><b>Note:</b> Use this to search and manage user accounts under your authority. You must select at least the <b>Application</b> to perform a search. Only the first 1,000 results will display.</i></p>	
<p>6a. If you are unable to locate a user in 'Application Search', you can select 'Enterprise Search', enter the user's details, and select <b>Search</b>.</p> <p><i><b>Note:</b> Use this to search and manage user accounts in the CMS Enterprise Portal. This search option is intended for helping users who may have called the wrong Help Desk or may not have an application role, etc. You must enter at least the <b>User ID</b> (or) <b>E-mail Address</b> (or) a combination of <b>First Name</b> (and) <b>Last Name</b> to perform a search. The results will only display if 10 or fewer results match the criteria.</i></p>	

## CMS Enterprise Portal QRG for Help Desk MFA Support

Steps	Screenshots
	
<p>7. Select <b>Manage MFA Device</b> from the 'Actions' drop-down list.</p> <p><i>Note: The option to select 'Manage MFA Device' is also available on the 'User Details' page.</i></p>	
<p>7a. Select the <b>User ID</b> to go to the 'User Details' page.</p>	


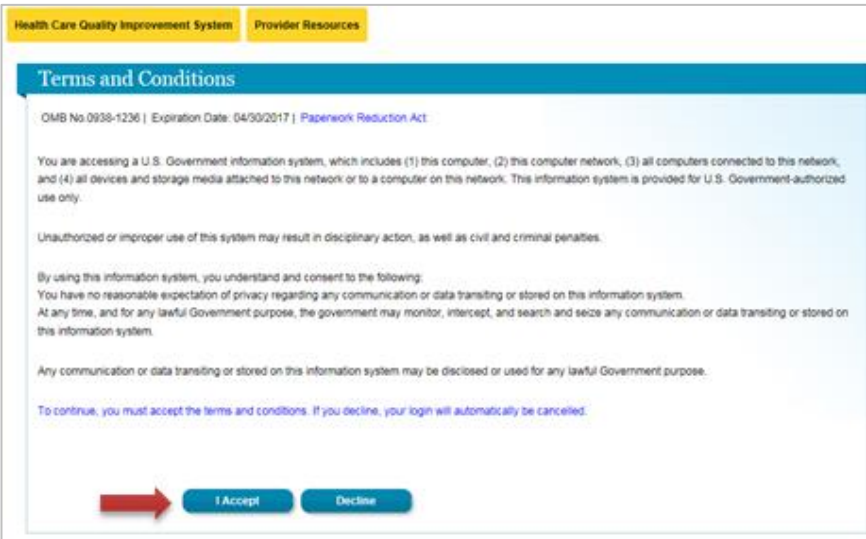
If you have questions or need assistance regarding MFA, please contact your Application Help Desk



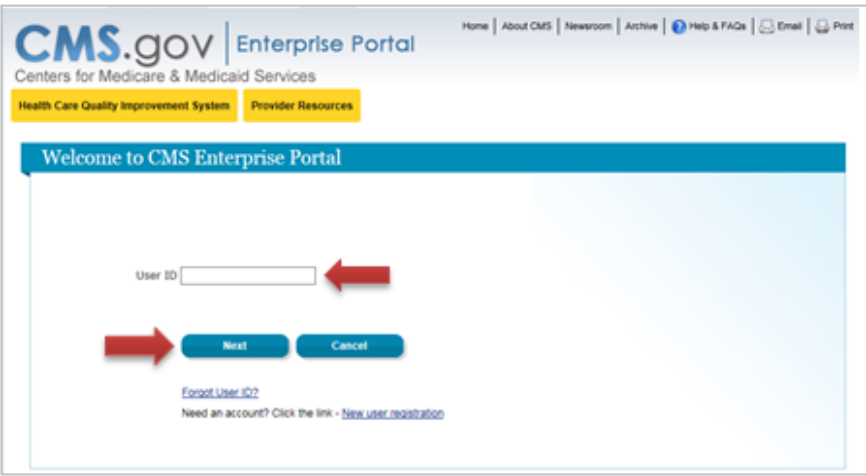
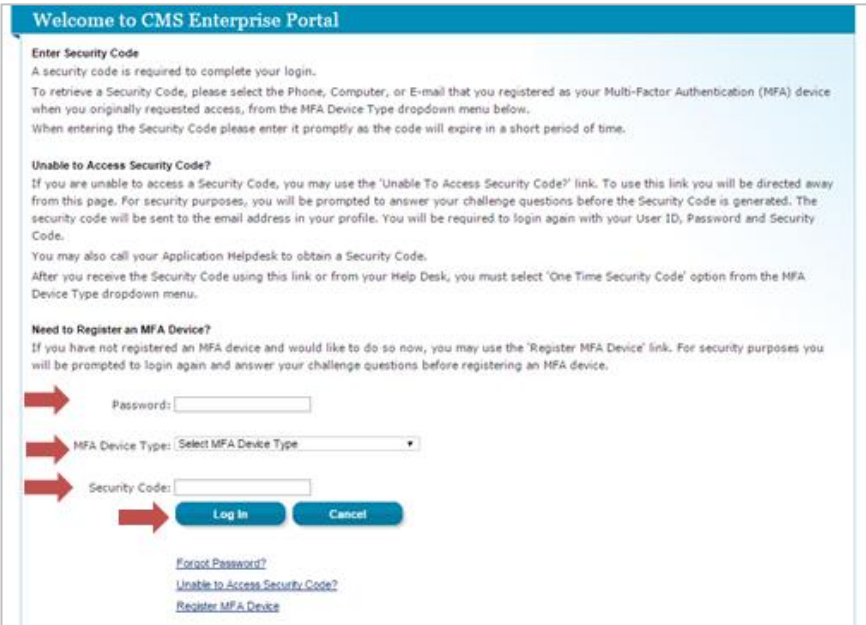
Steps	Screenshots
7b. Select <b>Manage MFA Device</b> .	
8. Select the checkbox corresponding to the MFA device that needs to be removed and select <b>Remove MFA Devices</b> .	
9. Select <b>OK</b> to confirm removing the registered MFA device.  OR  Select <b>Cancel</b> to return to the 'Manage MFA Device' page.	
10. A success message displays. Select <b>OK</b> to return to the search results.	

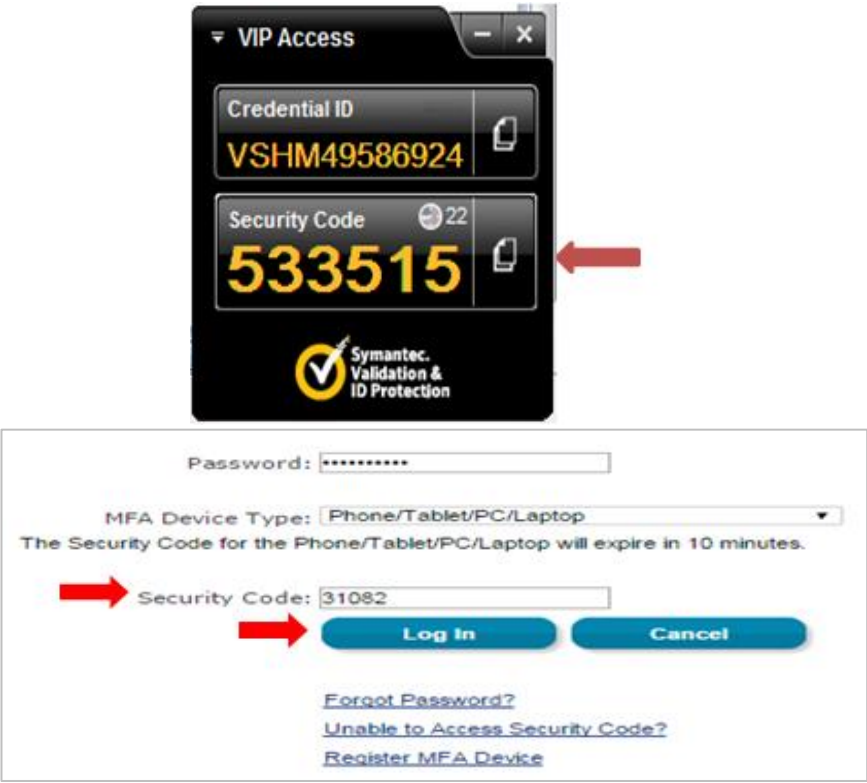

## 4. Step-by-Step Instructions to Generate One-Time Security Code

This section outlines the steps Application Help Desk Users, Application Approvers, and EIDM Help Desk Users take to generate a one-time MFA security code. Please follow each step listed below unless otherwise noted.

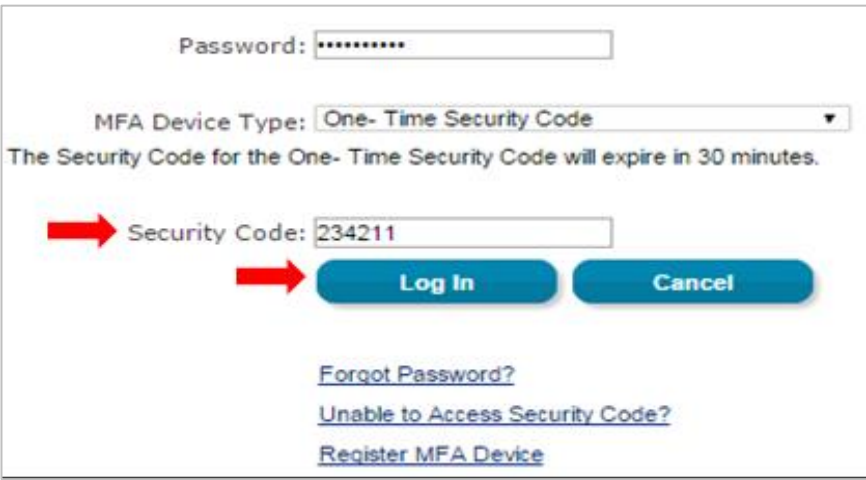
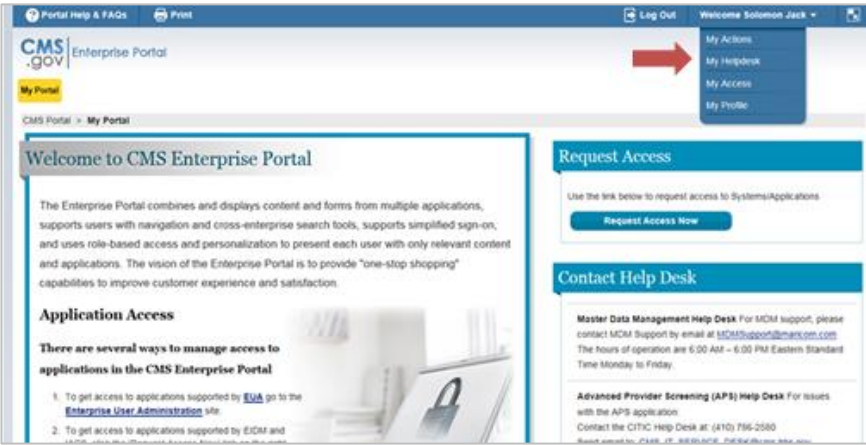
Steps	Screenshots
<p>1. Go to <a href="https://portal.cms.gov/">https://portal.cms.gov/</a> and select <b>Login to CMS Secure Portal</b> on the CMS Enterprise Portal.</p> <p><i>Note: The CMS Enterprise Portal supports the following browsers: Internet Explorer 11, Firefox, Chrome, and Safari.</i></p>	
<p>2. Read the 'Terms and Conditions' page and select <b>I Accept</b> to continue.</p>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

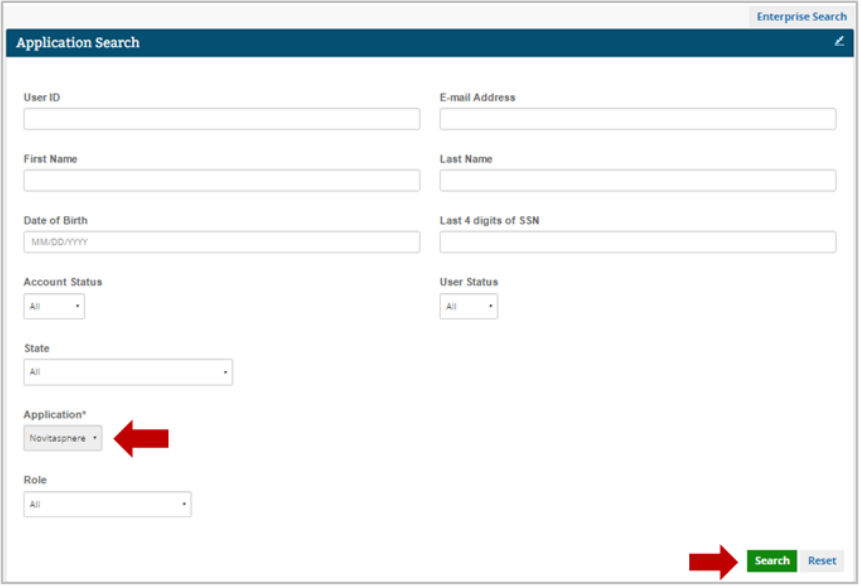
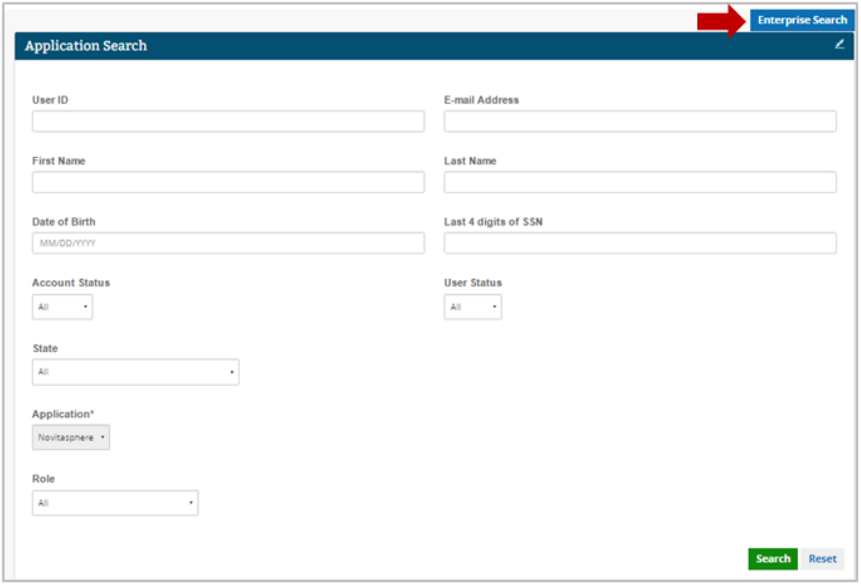
Steps	Screenshots
<p>3. Enter your <b>User ID</b> and select <b>Next</b>.</p>	
<p>4. Enter your <b>Password</b>, select an <b>MFA Device Type</b> from the drop-down list, enter the <b>Security Code</b>, and select <b>Log In</b>.</p> <p><i>Note: The 'Security Code' for the 'E-mail' and 'One-Time Security Code' options expires after 30 minutes. The 'Security Code' for the other MFA device types expires after 10 minutes. If you are unable to enter the code within the period, you will need to request a new one.</i></p> <p><i>If you do not have access to your registered MFA device, please refer to the 'User Login' QRG for step-by-step instructions on how to register an MFA Device.</i></p>	

Steps	Screenshots
<p>4a. If you select <b>Phone/Tablet/PC/Laptop</b> as the 'MFA Device Type', enter the VIP Access software's 'Security Code' as the MFA <b>Security Code</b> and select <b>Log In</b>.</p>	
<p>4b. If you select <b>Text Message – Short Message Service (SMS)</b>, <b>Interactive Voice Response (IVR)</b>, or <b>E-mail</b> as the 'MFA Device Type', select <b>Send</b> to receive the code on the selected MFA device type.</p> <p>Enter the <b>Security Code</b> and select <b>Log In</b>.</p>	

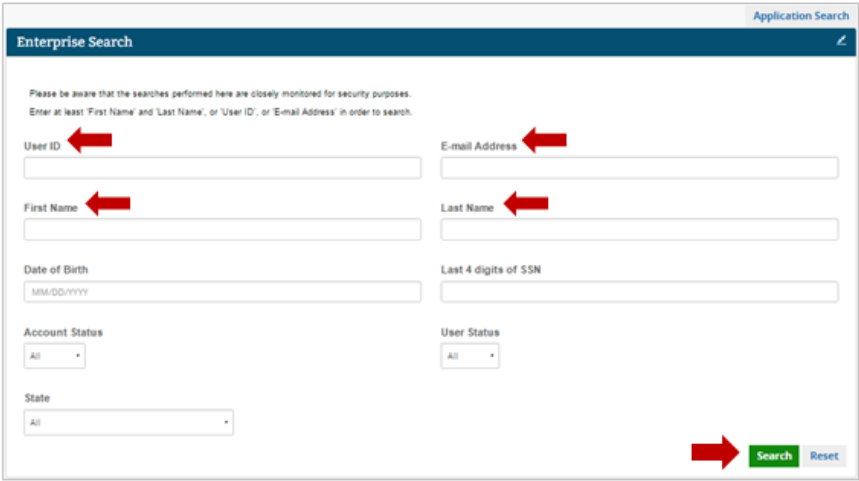
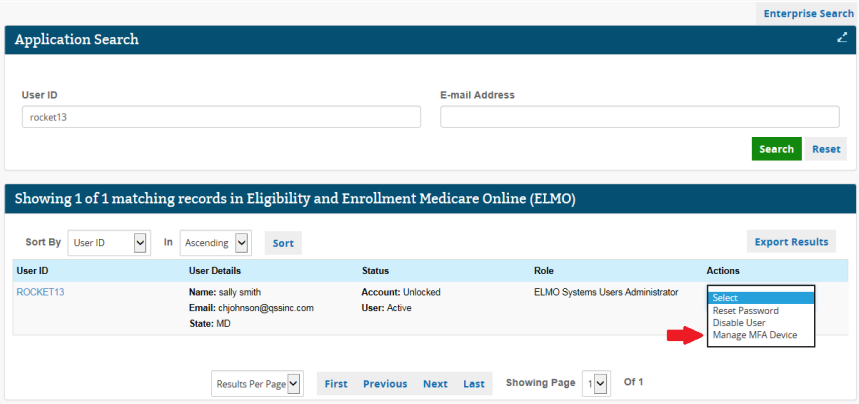
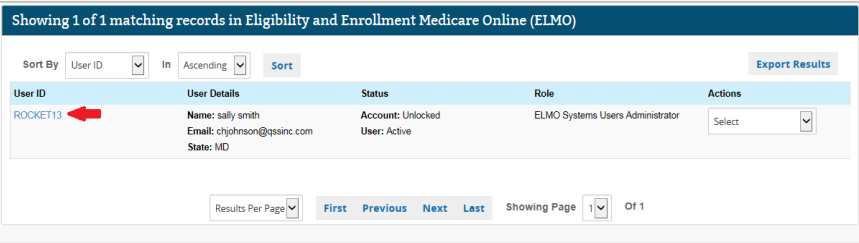
## CMS Enterprise Portal QRG for Help Desk MFA Support

Steps	Screenshots
<p>4c. If you select <b>One-Time Security Code</b> as the 'MFA Device Type', enter the code you receive either in the e-mail sent to your registered e-mail address via the 'Unable to Access Security Code?' link or from your Application Help Desk in the <b>Security Code</b> field and select <b>Log In</b>.</p>	
<p>5. Locate the 'Welcome &lt;First&gt; &lt;Last&gt;' drop-down list in the top-right corner of the page and select <b>My Helpdesk</b>.</p>	

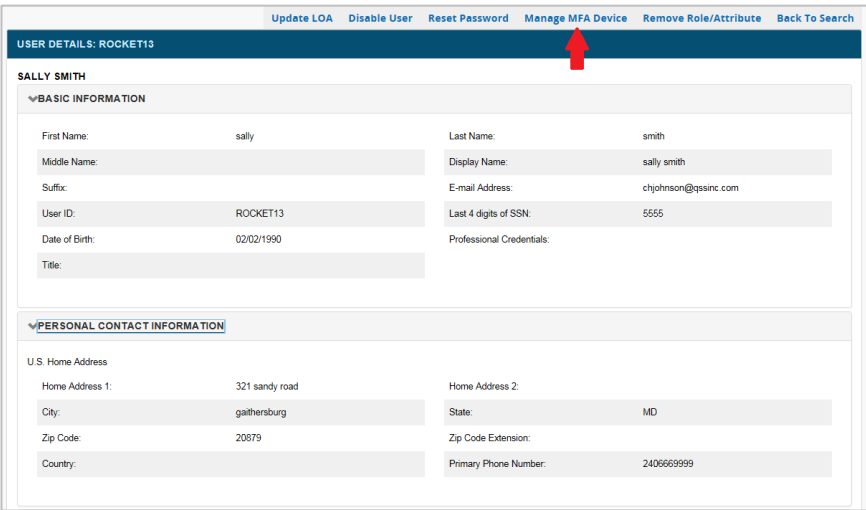
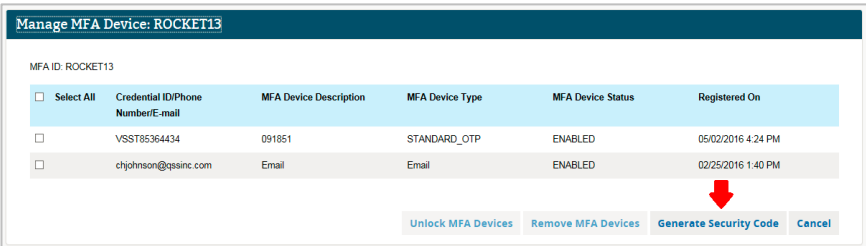
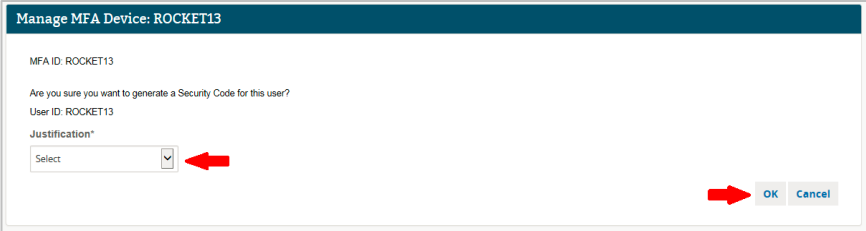
If you have questions or need assistance regarding MFA, please contact your Application Help Desk

Steps	Screenshots
<p>6. Enter the user's details on the 'Application Search' page and select <b>Search</b>.</p> <p><i><b>Note:</b> Use this to search and manage user accounts under your authority. You must select at least the <b>Application</b> to perform a search. Only the first 1,000 results will display.</i></p>	
<p>6a. If you are unable to locate a user in 'Application Search', you can select 'Enterprise Search', enter the user's details, and select <b>Search</b>.</p> <p><i><b>Note:</b> Use this to search and manage user accounts in the CMS Enterprise Portal. This search option is intended for helping users who may have called the wrong Help Desk or may not have an application role, etc. You must enter at least the <b>User ID</b> (or) <b>E-mail Address</b> (or) a combination of <b>First Name</b> (and) <b>Last Name</b> to perform a search. The results will only display if 10 or fewer results match the criteria.</i></p>	

## CMS Enterprise Portal QRG for Help Desk MFA Support

Steps	Screenshots
	
<p>7. Select <b>Manage MFA Device</b> from the 'Actions' drop-down list.</p> <p><i>Note: The option to select 'Manage MFA Device' is also available on the 'User Details' page.</i></p>	
<p>7a. Select the <b>User ID</b> to go to the 'User Details' page.</p>	

If you have questions or need assistance regarding MFA, please contact your Application Help Desk

Steps	Screenshots
7b. Select <b>Manage MFA Device</b> .	
<p>8. Select <b>Generate Security Code</b>.</p> <p><i>Note: The <b>Generate Security Code</b> button will be displayed only if the user has an MFA ID. It is not required to select the checkbox corresponding to an MFA device in order to generate a Security Code.</i></p>	
<p>9. Select a <b>Justification</b> from the drop-down list and select <b>OK</b>.</p> <p><i>Notes: The Justification values are:</i></p> <ul style="list-style-type: none"> <li><b>Unable to access device(s)</b> - Use when the user is unable to access their MFA device.</li> <li><b>No device registered</b> - Use when user does not have any registered MFA devices.</li> <li><b>Issue retrieving Security Code</b> - Use when the user is unable to retrieve the Security Code via any of the registered MFA devices.</li> </ul>	



Steps	Screenshots
10. Select the <b>Security Code Provided to User by Phone</b> checkbox if you gave the user the code over the phone and select <b>OK</b> to return to the search results page.	